(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－322280
（P2000－322280A）
(43)公開日　平成12年11月24日(2000.11.24)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｇ０６Ｆ　11/10	３３０	Ｇ０６Ｆ　11/10	３３０Ｑ	５Ｂ００１
Ｈ０３Ｍ　13/00		Ｈ０３Ｍ　13/00		５Ｊ０６５
Ｈ０４Ｌ　1/00		Ｈ０４Ｌ　1/00	Ｚ	５Ｋ０１４

審査請求　未請求　請求項の数２　ＯＬ　（全　４　頁）

(21)出願番号　特願平11－130903

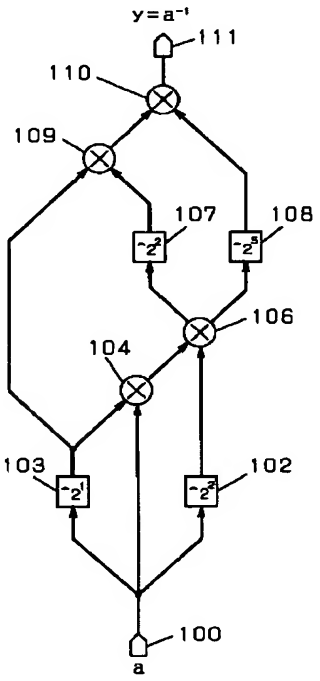
(22)出願日　平成11年５月12日(1999.5.12)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　花木　義孝
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100097445
弁理士　岩橋　文雄　（外２名）

Ｆターム(参考)　5B001 AA11 AB02 AC01
5J065 AC01 AD11 AF01 AF03 AG01 AH03
5K014 AA05 BA08 EA01 EA02

(54)【発明の名称】　ガロア体演算方法

(57)【要約】
【課題】　ガロア体の逆元を生成するガロア体演算器を実現するにあたり、高速なパイプライン動作を実現しつつ、回路規模の小さなガロア体演算器を実現することを目的とする。
【解決手段】　図１に示すようなガロア体演算の乗算器によるランダムロジックによって、逆元ＲＯＭを用いることなく、ガロア体ＧＦ（２＾８）上の逆元を生成する。これにより、ＲＭＯを用いることがないので、スループットの高い、高速なガロア体演算をすることができるという効果がある。



1

【特許請求の範囲】
【請求項１】　第１のガロア体の元を２乗して第２のガロア体の元を生成するステップと、
前記第１のガロア体の元を４乗して第３のガロア体の元を生成するステップと、
前記第１、第２のガロア体の元とをガロア体乗算して第４のガロア体の元を生成するステップと、
前記第３、第４のガロア体の元とをガロア体乗算して第５のガロア体の元を生成するステップと、
前記第５のガロア体の元を４乗して第６のガロア体の元を生成するステップと、
前記第５のガロア体の元を３２乗して第７のガロア体の元を生成するステップと、
前記第２、第６のガロア体の元とをガロア体乗算して第８のガロア体の元を生成するステップと、
前記第７、第８のガロア体の元とをガロア体乗算して前記第１のガロア体の元の逆元を生成するステップとを備えることを特徴とするガロア体演算方法。
【請求項２】　請求項１記載のガロア体演算方法において、
第１０のガロア体の元を入力し、第２のガロア体の元とガロア体乗算を行い、新たな第２のガロア体の元を生成するガロア体乗算ステップを更に備えることを特徴とするガロア体演算方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】蓄積装置、情報通信などの分野において、誤り訂正符号に関する技術の応用が盛んである。本発明は、誤り訂正符号として有力なリード・ソロモン符号の復号・符号化に必要となる、ガロア体演算方法に関するものである。
【０００２】
【従来の技術】従来、ガロア体ＧＦ（２＾ｎ）上の逆元生成器は、逆元ＲＯＭと呼ばれるＲＯＭを用いて構成されていた。逆元ＲＯＭには、ガロア体上の逆元がデータとして格納されている。
【０００３】図２に、従来のガロア体上の逆元生成器の構成を示す。図２において、１００は入力端子、１１１は出力端子、１１２は逆元ＲＯＭである。
【０００４】図３の構成によるガロア体逆元生成器の動作を、以下に説明する。まず、ガロア体演算方法への入力が逆元ＲＯＭ１１２に入力され、その逆元が逆元ＲＯＭ１１２から出力され、端子１１１から出力される。
【０００５】従来の構成では、以上のようにして、ガロア体逆元生成器を得ていた。
【０００６】図４に、従来のガロア体除算器の構成を示す。図４において、１００、１０１は入力端子、１１１は入力端子、１１２は端子１０１から入力されたガロア体ＧＦ（２＾８）上の逆数を出力する逆元ＲＯＭ、１１４は端子１１０からの入力と逆元ＲＯＭ１１２の出力を

2

乗ずるガロア体乗算器である。
【０００７】図４の構成によるガロア体除算器の動作を、以下に説明する。まず、ガロア体演算方法へ除数として与えられた入力ｂが逆元ＲＯＭ１１２に入力され、その逆元ｂ＾（－１）が逆元ＲＯＭ１１２から出力される。ガロア体乗算器１１４では、逆元ＲＯＭから出力された除数の逆元ｂ＾（－１）と端子１００から入力された被除数ａとを乗ずることによってガロア体除算の結果ｂ／ａが生成され、端子１１１から出力される。
【０００８】従来の構成では、以上のようにして、ガロア体除算器を得ていた。
【０００９】
【発明が解決しようとする課題】以下に、従来のガロア体演算方法の構成における課題について論ずる。従来の構成では、ガロア体上の逆元を生成するため、あるいは、ガロア体上の除算を実行するためには、ガロア体上の逆元を記憶したＲＯＭが必要であった。そのため、ガロア体演算方法にパイプライン構造をもたせて、ＲＯＭのアクセス速度以上のスループットを実現するには、複数のＲＯＭをインターリーブさせる必要があり、高速なパイプライン動作を実現しつつ回路規模の小さなガロア体演算方法を得るのが困難である、という課題があった。また、ガロア体の原始多項式に対応した逆元ＲＯＭが必要であるため、複数の原始多項式に対応するためには、原始多項式の数と同数の逆元ＲＯＭが必要となる。そのため、複数の原始多項式に対応しつつ回路規模の小さなガロア体演算方法を得るのが困難である、という課題があった。また、ガロア体上の逆元を記憶するための専用ＲＯＭを実装する必要があるため、ゲートアレイやＦＰＧＡなどに実装するのが困難である、という課題があった。
【００１０】本発明は、上記のような従来の課題を解決するものであり、ガロア体上の逆元の生成、あるいは、ガロア体上の除算をおこなうガロア体演算方法を実現するにあたり、高速なパイプライン動作を実現しつつ回路規模の小さなガロア体演算方法を提供すること、および、複数の原始多項式に対応しつつなお回路規模の小さなガロア体演算方法を提供すること、および、ゲートアレイやＦＰＧＡなどにも容易に実装可能なガロア体演算方法を提供することを目的とする。
【００１１】
【課題を解決するための手段】この目的を達成するために、本発明の請求項１、および請求項２記載のガロア体演算方法は、ガロア体ＧＦ（２＾８）上の元を入力する端子と、ガロア体２乗回路と、ガロア体４乗回路と、ガロア体３２乗回路と、４つのガロア体乗算回路と、出力端子とで構成されることを特徴とする。
【００１２】この構成では、回路がランダムロジックで構成されるため、容易にガロア体演算方法にパイプライン構造を持たせることができる。すなわち、スループッ

トの高いガロア体演算パイプラインを実現可能である。

【００１３】また、この構成では、逆元ＲＯＭを必要とせず、回路面積の大部分はガロア体乗算器で占められるが、ガロア体乗算器は回路規模をさほど増大させることなく対応する原始多項式の数を増加させ得る。このため、複数の原始多項式に対応しつつ、回路面積の小さなガロア体演算方法を構成することが可能である。

【００１４】また、この構成では、逆元ＲＯＭを必要とせず、ゲートアレイやＦＰＧＡへの実装が容易である。

【００１５】

【発明の実施の形態】以下、本発明の実施の形態について、図面を参照しながら説明する。

【００１６】（実施の形態１）図１は、本実施の形態１のガロア体演算方法の構成を示すブロック図である。図１のガロア体演算方法は、ガロア体上の逆元を生成する。

【００１７】図１において、１００はガロア体ＧＦ（２＾８）上の元ａを入力する端子、１０２は端子１００からの入力ａを４乗するガロア体４乗回路、１０３は端子１００からの入力ａを２乗するガロア体２乗回路、１０４は端子１００からの入力ａとガロア体２乗回路１０３からの出力（ａ＾４）を乗ずるガロア体乗算器、１０６はガロア体４乗回路１０２からの出力（ａ＾４）とガロア体乗算器１０４からの出力（ａ＾３）を乗ずるガロア体乗算器、１０７はガロア体乗算器１０６の出力（ａ＾７）を４乗するガロア体４乗回路、１０８はガロア体乗算器１０６の出力（ａ＾７）を３２乗するガロア体３２乗回路、１０９はガロア体２乗回路１０３の出力（ａ＾２）とガロア体４乗回路１０７の出力（ａ＾２８）を乗ずるガロア体乗算器、１１０はガロア体３２乗回路１０８の出力（ａ＾２２４）とガロア体乗算器１０９の出力（ａ＾３０）を乗ずるガロア体乗算器、１１１はガロア体乗算器１１０の出力（ａ＾２５４＝ａ＾（－１））を出力する端子である。

【００１８】以上のように構成された実施の形態１のガロア体演算方法の動作を、以下に説明する。まず、ガロア体ＧＦ（２＾８）上の元ａが端子１００から入力され、ガロア体４乗回路１０２においてａ＾４が生成され、ガロア体２乗回路１０３においてａ＾２が生成され、ガロア体乗算器１０４においてａ＾３が生成され、ガロア体乗算器１０６においてａ＾７が生成され、ガロア体４乗回路１０７においてａ＾２８が生成され、ガロア体３２乗回路１０８においてａ＾２２４が生成され、ガロア体乗算器１０９においてａ＾３０が生成され、ガロア体乗算器１１０においてａ＾２５４が生成され、端子１１１から出力される。これはガロア体演算方法の入力ａの逆数ａ＾（－１）に等しい。

【００１９】以上のようにして、本発明の実施の形態１のガロア体演算方法では、ガロア体ＧＦ（２＾８）上の逆数を得る。

【００２０】ここで、以上の構成において、演算遅延を考慮して、適切な場所にラッチを挿入することにより、パイプライン動作をさせ、スループットを向上させることができる。よって逆元ＲＯＭを用いた場合に比べ、スループットは向上するという効果がある。

【００２１】（実施の形態２）図２は、本実施の形態２のガロア体演算方法の構成を示すブロック図である。図２のガロア体演算方法は、ガロア体ＧＦ（２＾８）上の除算をおこなう。

【００２２】図２において、１００はガロア体ＧＦ（２＾８）上の元ａを入力する端子、１０１はガロア体ＧＦ（２＾８）上の元ｂを入力する端子、１０２は端子１００からの入力ａを４乗するガロア体４乗回路、１０３は端子１００からの入力ａを２乗するガロア体２乗回路、１０４は端子１００からの入力ａとガロア体２乗回路１０３からの出力（ａ＾４）を乗ずるガロア体乗算器、１０５は端子１０１からの入力ｂとガロア体乗算器１０３の出力（ａ＾２）とを乗ずるガロア体乗算器、１０６はガロア体４乗回路１０２からの出力（ａ＾４）とガロア体乗算器１０４からの出力（ａ＾３）を乗ずるガロア体乗算器、１０７はガロア体乗算器１０６の出力（ａ＾７）を４乗するガロア体４乗回路、１０８はガロア体乗算器１０６の出力（ａ＾７）を３２乗するガロア体３２乗回路、１０９はガロア体２乗回路１０３の出力（ａ＾２）とガロア体４乗回路１０７の出力（ａ＾２８）を乗ずるガロア体乗算器、１１０はガロア体３２乗回路１０８の出力（ｂｘａ＾２２４）とガロア体乗算器１０９の出力（ｂｘａ＾３０）を乗ずるガロア体乗算器、１１１はガロア体乗算器１１０の出力（ｂｘａ＾２５４＝ｂ／ａ）を出力する端子である。

【００２３】以上のように構成された実施の形態１のガロア体演算方法の動作を、以下に説明する。まず、ガロア体ＧＦ（２＾８）上の元ａが端子１００から入力され、ガロア体４乗回路１０２においてａ＾４が生成され、ガロア体２乗回路１０３においてａ＾２が生成され、ガロア体乗算器１０４においてａ＾３が生成され、ガロア体乗算器１０５においてｂｘａ＾２が生成され、ガロア体乗算器１０６においてａ＾７が生成され、ガロア体４乗回路１０７においてａ＾２８が生成され、ガロア体３２乗回路１０８においてａ＾２２４が生成され、ガロア体乗算器１０９においてｂｘａ＾３０が生成され、ガロア体乗算器１１０においてｂｘａ＾２５４が生成され、端子１１１から出力される。これはｂ／ａに等しい。

【００２４】以上のようにして、本発明の実施の形態２のガロア体演算方法では、ガロア体ＧＦ（２＾８）上の除算をおこなう。

【００２５】ここで、以上の構成において、演算遅延を考慮して、適切な場所にラッチを挿入することにより、パイプライン動作をさせ、スループットを向上させるこ

5

とができる。よって逆元ＲＯＭを用いた場合に比べ、スループットは向上するという効果がある。

【００２６】

【発明の効果】以上のように、本発明によれば、入力する端子と、ガロア体２乗回路と、ガロア体４乗回路と、ガロア体３２乗回路と、５つのガロア体乗算回路と、出力端子とを備えることにより、容易にパイプライン化が可能で、回路規模を増大させることなく複数の原始多項式に対応可能で、ゲートアレイやＦＰＧＡへの実装も容易なガロア体演算方法を得ることができる。

【図面の簡単な説明】

【図１】本発明の実施の形態１に係るガロア体逆元生成器の構成を示すブロック図

【図２】本発明の実施の形態２に係るガロア体除算器の構成を示すブロック図

6

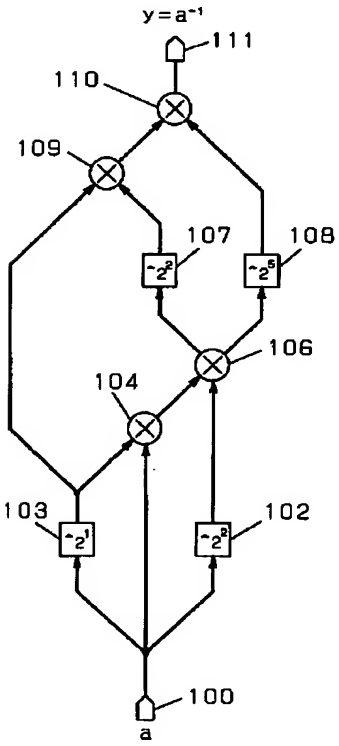
*【図３】従来のガロア体逆元生成器の構成を示すブロック図

【図４】従来のガロア体除算器の構成を示すブロック図

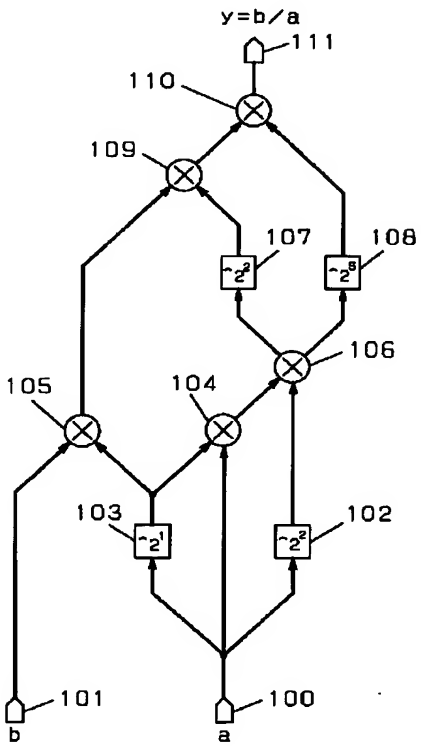
【符号の説明】

１００～１０１　入力端子
１０２　ガロア体４乗回路
１０３　ガロア体２乗回路
１０４～１０６　ガロア体乗算器
１０７　ガロア体４乗回路
１０８　ガロア体３２乗回路
１０９～１１０　ガロア体乗算器
１１１　出力端子
１１２　逆元ＲＯＭ
１１４　ガロア体乗算器

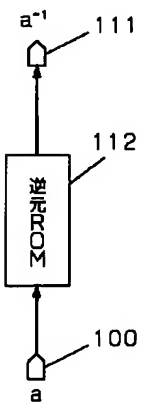
【図１】



【図２】



【図３】



【図４】